Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A computer network comprising:

a first edge device coupled to a first physical private network, the first edge device configured to create a first table with information of a group of one or more virtual private networks reachable through the first edge device, the first table being stored in a first database;

a second edge device coupled to a second physical private network, the second edge device configured to create a second table with information of the group of one or more virtual private networks reachable through the second edge device, the second table being stored in a second database;

wherein, the first and second edge devices enable secure communication between the first and second physical private networks, and the first edge device shares the information of the group of one or more virtual private networks of the first table with the second edge device and the second edge device shares the information of the group of one or more virtual private networks of the second table with the first edge device; and

wherein communication between the first and second physical private networks is managed according to a security policy associated with the first and second physical private networks, wherein the security policy is defined for a security policy group comprising one or more virtual private networks having a hierarchical organization, users allowed to access the virtual private networks, and a rule controlling access to the virtual private networks.

Claims 2-6 (canceled)

Claim 7 (currently amended): The computer network of claim 1 [[6]], wherein each of the one or more virtual private networks has full connectivity with all other virtual private networks and the security policy defined for the security policy group is automatically configured for each connection.

Claim 8 (currently amended): The computer network of claim 1 [[6]], wherein the security policy provides encryption of traffic among the one or more virtual private networks and the rule is a firewall rule providing access control of the encrypted traffic among the one or more virtual private networks.

Claim 9 (currently amended): In a computer network including a first edge device coupled to a first physical private network and a second edge device coupled to a second physical private network, the first and second edge devices enabling secure communication between the first and second physical private networks, a method for gathering virtual private network membership information comprising:

defining a security policy for a security policy group, the security policy group comprising one or more virtual private networks having a hierarchical organization, users allowed to access the one or more virtual private networks, and a rule controlling access to the one or more virtual private networks;

creating a first table with information of a group of one or more virtual private networks reachable through the first edge device,

storing the first table in a first database;

creating a second table with information of the group of one or more virtual private networks reachable through the second edge device;

storing the second table in a second database;

sharing the information of the group of one or more virtual private networks of the first table with the second edge device; and

sharing the information of the group of one or more virtual private networks of the second table with the first edge device;

wherein communication between the first and second physical private networks is managed according to the security policy associated with the first and second physical private networks.

Claims 10-14 (canceled)

Claim 15 (currently amended): The method of claim 9 [[14]], wherein each of the one or more virtual private networks has full connectivity with all other virtual private networks and the security policy defined for the security policy group is automatically configured for each connection.

Claim 16 (currently amended): The method of claim 9 [[14]], wherein the security policy provides encryption of traffic among the virtual private networks and the rule is a firewall rule providing access control of the encrypted traffic among the virtual private networks.